| NODIS Library | Program Management(8000s) | Search |

**NASA
Procedural
Requirements**

NPR 8715.3D
Effective Date: December 16, 2021
Expiration Date: December 21, 2026

COMPLIANCE IS MANDATORY FOR NASA EMPLOYEES

Printable Format (PDF)

Subject: NASA General Safety Program Requirements

Responsible Office: Office of Safety and Mission Assurance

Chapter 1. Programmatic Safety Requirements

1.1 Overview of the NASA Safety Program

1.1.1 This document provides the procedural requirements that define the NASA Safety Program. Safety program responsibility starts at the top with senior management's role of developing policies and providing strategies and resources necessary to implement and manage a comprehensive safety program. The NASA Safety Program is executed by the responsible Mission Directorate Associate Administrators, Center Directors, Office of Safety and Mission Assurance (OSMA), component facility managers, safety managers, project managers, systems engineers, supervisors, line organizations, employees, and NASA contractors.

Note: The basic principles for governing, managing, implementing, monitoring, and controlling work at NASA are addressed in NPD 1000.0, which provides direction for Mission Directorates and Centers to execute programs and projects.

1.1.2 As stated in NPD 8700.1, the objectives of the NASA Safety Program are to protect the public from harm, ensure the safety of employees, and affect positively the overall success rate of missions and operations through preventing damage to high-value equipment and property.

1.1.3 In general, the success or failure of an organization's safety efforts can be predicted by a combination of leading indicators (e.g., the number of open vs. closed inspection findings, awareness campaigns, training metrics, progress towards safety goals/objectives, the amount of hazard and safety analyses completed, and close calls) and its achievement measured by lagging indicators (e.g., the number of incidents involving injury or death to personnel, lost productivity [lost or restricted workdays], environmental damage, or loss of, or damage to, property). Like many successful corporations, NASA has learned that aggressively preventing mishaps is good management and a sound business practice.

1.1.4 NASA undertakes many activities involving high risk. Management of this risk is one of NASA's most challenging activities and is an integral part of NASA's safety efforts.

1.1.5 Policies, requirements, and procedures for mishap investigations are provided in NPR 8621.1.

1.1.6 NASA identifies issues of concern through a strong network of oversight councils and internal auditors including the Aerospace Safety Advisory Panel (ASAP).

1.1.7 NASA's goal is to maintain a world-class safety program based on management and employee commitment and involvement; system and worksite safety and risk assessment; hazard and risk prevention, mitigation, and control; and safety and health training.

1.2 NASA General Safety Program Roles and Responsibilities

Per NPD 1000.3, Mission Directorate Associate Administrators, through their project managers, and Center Directors, through their line managers, are responsible for the safety of the public and of their assigned personnel, facilities, and mission systems from hazards created or controlled by the Mission Directorate or Center. Toward that end, they shall establish a safety and health program in accordance with NPR 8715.1, NASA Safety and Health Programs and meet the requirements of this NPR.

1.3 Public Safety

Mission Directorate Associate Administrators and Center Directors shall ensure operational safety in accordance with NPR 8715.1.

1.4 Institutional Roles and Responsibilities in the NASA Safety Program - *RESERVED*

1.5 Program Management Roles and Responsibilities in the NASA Safety Program

1.5.1 Mission Directorate Associate Administrators shall ensure that program and project Safety and Mission Assurance (SMA) Plans:

a. Addresses life cycle safety-relevant functions and activities.

b. Reflects a life cycle SMA process perspective, addressing areas including: procurement, management, design and engineering, design verification and test, software design, software verification and test, manufacturing, manufacturing verification and test, operations, and preflight verification and test.

c. Contains data and information to support each section of the SMA Plan for each major milestone review to include the Safety and Mission Success Review.

d. Contains trending and metrics utilized to display progress and to predict growth towards SMA goals and requirements.

e. As a minimum, addresses the following topics and associated requirements:

(1) Safety and mission success per this NPR.

(2) Risk classification of NASA payloads per NPR 8705.4.

(3) Reliability and maintainability per NPD 8720.1.

(4) Risk assessment per NPR 8705.5.

(5) Quality assurance per NPR 8735.2.

(6) Software safety and assurance per and NASA-STD-8739.8.

(7) Public and workforce safety and health per host Center requirements and consistent with NPR 8715.1.

(8) Range safety per per host Center requirements and consistent with NPR 8715.5.

(9) Payload safety per host Center requirements and consistent with NPR 8715.7.

(10) Orbital debris mitigation requirements per NPR 8715.6.

(11) Planetary protection requirements per NPR 8020.12, NID 8715.128, and NID 8715.129.

(12) Nuclear flight safety per chapter 6 of this NPR.

(13) Human-rating per NPR 8705.2.

(14) Mishap reporting per NPR 8621.1.

(15) Compliance verification, SMA audits, reviews, and assessments per NPR 8705.6.

1.5.2 Project managers shall ensure that contractor operations and designs are evaluated for consistency and compliance with the safety and health provisions provided in their contractual agreements.

1.6 Risk Assessment and Risk Acceptance

Requirements for risk assessment and acceptance are addressed as part of risk management in NPR 8000.4, Agency Risk Management Procedural Requirements.

1.7 Technical Safety Requirements for NASA-Unique Designs and Operations

1.7.1 Risk Reduction Protocol

1.7.1.1 Project managers shall ensure that hazards and dominant contributors to risk are controlled according to the following:

a. Eliminate accident scenarios (e.g., eliminate hazards or initiating events by design).

b. Reduce the likelihood of accident scenarios through design and operational changes (hazard control).

c. Reduce the severity of accident consequences (hazard mitigation).

d. Improve the state-of-knowledge regarding key uncertainties that drive the risk associated with a hazard (uncertainty reduction to support implementation of the above strategies).

> *Note: Designs for hazard control and accident prevention and mitigation should include considerations for the possibility of human errors. The level of hazard control should be based on the level of risk associated with that hazard. Examples of risk reduction strategies include: control of system and operational characteristics, incorporation of safety devices, use of caution and warning devices, and the use of operational and management procedures and training. Some hazards may require a combination of several of these approaches for prevention, mitigation, and/or control. Providing protective clothing and equipment is considered an operational procedure.*

1.7.2 Reliability and Failure Tolerance

1.7.2.1 Safety critical operations must have high reliability. High reliability is verified by reliability analysis using accepted modeling techniques and data in which uncertainties are incorporated. Where this cannot be accomplished with a specified confidence level, the design of safety critical operations shall have failure tolerance and safety margins in which critical operability and functionality are ensured. Failure tolerance is the ability of a system to perform its function(s) or maintain control of a hazard in the presence of failures of its subsystems. Failure tolerance may be accomplished through like or unlike redundancy. Safety margins are the difference between as-built factor of safety and the ratio of actual operating conditions to the maximum operating conditions specified during design.

> Note: For human space systems, failure tolerance requirements are provided in NPR 8705.2. Applicable failure tolerance requirements in this NPR pertain to all other systems.

1.7.2.2 To assure operability and functionality and to achieve failure tolerance, project managers shall use these design considerations.

a. Design safety critical systems such that the critical operation or its necessary functions can be assured. To provide assurance, design the component, subsystem, or system so it is are capable of being tested, inspected, and maintained.

b. Where high reliability cannot be verified by reliability analysis using accepted data in which uncertainties are incorporated, design safety critical systems so that no combination of two failures and/or operator errors (fail-safe, fail-safe as a minimum) will result in loss of life.

> Note: Safety-critical operational controls are applied to conditions, events, signals, processes, or items for which proper recognition, control, performance, or tolerance are essential to safe system operation, use, or function.

c. Where high reliability cannot be verified by reliability analysis using accepted data in which uncertainties are incorporated, design safety critical operations so that no single failure or operator error (fail-safe) will result in system loss/damage or personal injury.

d. Where high reliability cannot be verified by reliability analysis using accepted data in which uncertainties are incorporated, provide functional redundancy where there is insufficient time for recovery or system restoration. Where there is sufficient time between a failure and the manifestation of its effect, design for restoration of safe operation using spares, procedures, or maintenance provides an alternative means of achieving failure tolerance.

e. Design safety critical systems and operations to have a safety margin.

f. When using redundancy, verify that common cause failures (e.g., contamination, close proximity) do not invalidate the assumption of failure independence.

g. When using redundancy in operations that could cause or lead to severe injury, major damage, or mission failure (safety critical operations), verify operability under conditions that singularly or separately added together represent the operating intended condition.

h.. When using reliability analyses, assess the probability of failure and associated uncertainties to provide the function and the time to restore the function, where loss of life, serious injury, or catastrophic system loss can occur. The time to restore the function shall include the active time to repair and the time associated with the logistics or administrative downtime that affects the ease or rapidity of achieving full restoration of the failed function.

1.7.2.3 To assure functional protection, project managers shall ensure that:

a. Loss of functional protection for safety-critical operations requires termination of the operation at the first stable configuration.

b. At least one single level of functional protection is used to protect high-value facilities and flight systems.

1.7.3 Inhibits

1.7.3.1 Where high reliability is not verified by reliability analysis using accepted data with uncertainties incorporated, the project manager shall ensure that:

a. Operations that require the control of a condition, event, signal, process, or item for which proper recognition, performance, or tolerance is essential to safe system operation, use, or function are designed such that an inadvertent or unauthorized event cannot occur (inhibit).

b. Operations have three inhibits where loss of life can occur.

c. Operations have two inhibits where personal injury, illness, mission loss, or system loss or damage can occur.

d. The capability of inhibits or control procedures when required in operations by this paragraph are verified under operational conditions including the verification of independence among multiple inhibits.

> *Note: Inhibits (designs that specifically prevent an inadvertent or unauthorized event from occurring) are not to be confused with the lockout/tagout program, which is a program to isolate or control facility system hazards; e.g., electrical, mechanical, hydraulic, pneumatic, chemical, thermal, or other energy.*

1.8 SMA Program Reviews

Requirements for conducting and supporting independent SMA audits, reviews, and assessments are provided in NPR 8705.6.

1.9 Advisory Panels, Committees, and Boards

The Aerospace Safety Advisory Panel and the Independent Verification and Validation Board of Advisors are addressed in NPD 1000.3.

1.10 Coordination with Organizations External to NASA - *RESERVED*

1.11 Safety Motivation and Awards Program - *RESERVED*

1.12 Safety Management Information - *RESERVED*

1.13 Tailoring Agency Mission SMA Requirements

1.13.1 This section is applicable to programs and projects governed by NPR 7120.5 and NPR 7120.8. Processes for tailoring Agency SMA requirements will follow the requirement tailoring principles defined in NPRs 7120.5 and 7120.8.

1.13.2 NPR 8715.1, NASA Safety and Health Programs, describes the process for tailoring institutional safety and health requirements.

1.13.3 The Chief, SMA delegates the authority to approve tailoring of Agency mission SMA requirements imposed on programs and projects, including the acceptance of alternate technical standards, to the Center-level SMA TA except for the following areas for which the Chief, SMA retains this authority:

a. Orbital debris mitigation, including requirements in NPR 8715.6, NASA Procedural Requirements for Limiting Orbital Debris and Evaluating the Meteoroid and Orbital Debris Environments, and standards incorporated by reference therein.

b. Planetary protection, including requirements in NPR 8715.24, Planetary Protection Provisions for Robotic Extraterrestrial Missions, NID 8715.129, Biological Planetary Protection for Human Missions to Mars, and agreed to standards used to implement those requirements.

c. Nuclear flight safety, including requirements in Chapter 6, Nuclear Safety for Launching of Radioactive Materials, and agreed to standards used to implement those requirements.

> *Note: This reference to Chapter 6 will be replaced with NPR 8715.yy, Nuclear Flight Safety, once the new NPR is published.*

d. Human-rating spaceflight systems, including requirements in NPR 8705.2, Human-Rating Requirements for Space Systems, excluding standards incorporated by reference therein.

e. Mission risk classification, including requirements in NPR 8705.4, Risk Classification for NASA Payloads, excluding standards incorporated by reference therein.

f. Mishap investigations, including requirements in NPR 8621.1, NASA Procedural Requirements for Mishap and Close Call Reporting, Investigating, and Recordkeeping.

g. NASA interim directives that replace or augment the documents cited above.

1.13.4 The Chief, SMA will consult on the tailoring of requirements in those areas with the Associate Administrator, Administrator, or other authorities as appropriate.

1.13.5 When tailoring requirements, the Mission Directorate Associate Administrator, or designee, shall include the following information in the request:

a. Identify the requirement(s) being tailored.

b. Describe the tailoring of the requirement (i.e., the nature of the proposed departure from the requirement).

c. Justify the reasons for the tailoring, why it is not possible, or desirable, to comply with the requirement .

d. Describe the resulting change in risk to the public, workforce, high-value property, and orbital and planetary environments.

e. Describe the resulting change in risk to crew safety and mission success.

f. Confirm the tailoring does not conflict with applicable Federal statutes or regulations, or with Agency policy or higher-level requirement.

g. Indicate when and whether compliance will be achieved.

h. Describe alternate actions to be taken for managing the risk.

i. Describe findings and recommendations from the project-level SMA TA regarding the technical merits of the case.

j. For matters involving human safety risk, obtain formal agreement to assume the risk from the actual risk taker(s) (or official spokesperson[s] and applicable supervisory chain).

1.13.6 NPR 8000.4 contains requirements for decisions to accept risk to safety and mission success.

1.14 Hazardous Work Activities That Are Outside NASA Operational Control

Note: Non-spaceflight activities are now addressed in NPR 8715.1, in particular section 4.3.10, Multiemployer Worksites - Worksites not under NASA control, and section 13.8, Test / Operations Safety, for requirements on NASA civil servant participation in hazardous work activities outside NASA operational control.

1.14 Hazardous Work Activities That Are Outside NASA Operational Control

1.14.1 It is NASA policy to formally review and approve NASA participation in hazardous work activities that are outside NASA operational control as needed to ensure that NASA safety and health responsibilities are satisfied. This policy applies unconditionally to NASA participation in commercial human spaceflight where current federal regulations do not necessarily provide for the safety of spaceflight vehicle occupants. This policy is non-retroactive and applies to hazardous ground or flight activities that involve research, development, test and evaluation, operations, or training, where all five of the following conditions exist:

a. NASA civil service personnel, Government detailees, specified contractors, or specified grantees are performing work for NASA.

Note 1: Paragraph 1.14 of this NPR applies to contractors and grantees only as specified by the responsible NASA manager in consultation with the cognizant NASA Center SMA organization based on an assessment of NASA safety responsibilities and/or obligations with regard to the activity.

Note 2: This policy only applies to personnel participating in activities within their official NASA duties.

b. The activity is outside NASA's direct operational control/oversight.

c. An assessment by the responsible NASA manager indicates there are insufficient safeguards and/or oversight in place.

Note: This policy does not apply to activities where safety oversight and/or safety regulations of other entities provide for safety of the participants (e.g., FAA, DoD, OSHA, ESA, JAXA) and foreign government-associated safety regulatory regimes.

d. The activity is not covered by a basic contract, grant, or agreement where Federal, State, and/or local requirements address personnel safety.

e. The nature of the activity is such that, if NASA were controlling it, a formal safety and/or health review would be required as part of the NASA approval process.

> *Note: Paragraph 1.14 of this NPR applies to activities conducted in unusual or unforgiving environments (such as underwater or extreme temperature/altitude), as well as activities conducted in remote areas where there is little or no access to medical care or other assistance in an emergency.*

1.14.2 For NASA work activities that satisfy the conditions listed in paragraph 1.14.1 of this NPR, it is NASA policy to document and verify that risks are adequately controlled and any residual risk is acceptable following the steps below or through implementation of the System Safety process in Chapter 2 of this NPR:

a. As early as practical, conduct a comprehensive, documented review of the planned activity (the review may address a series of related activities). (See paragraph 1.14.3.h of this NPR for requirements that apply to the review.)

b. Document Agency approval by cognizant NASA officials, including formal acceptance of all associated risks.

c. Ensure activity participants are fully briefed on the safety and health aspects of the activity and the associated risks and that they formally consent to take the risk.

d. Ensure activity participants have all necessary training, equipment, and support.

1.14.3 Roles and Responsibilities. The following roles and responsibilities apply with regard to implementing the policy stated in paragraph 1.14.2 of this NPR.

a. The Chief, Safety and Mission Assurance shall oversee and resolve any questions regarding the implementation and applicability of this policy and related requirements to a proposed work activity.

b. Each Center Safety and Mission Assurance Director shall:

(1) Establish and implement processes and requirements needed to ensure compliance with this policy for applicable work activities within the scope of their authority.

(2) Provide safety expertise as needed to assist programs and projects to successfully complete the required NASA review and approval of applicable work activities.

(3) Formally concur in the scope of hazard assessments executed per paragraph 1.14.3.h.(2) for activities under their cognizance.

(4) Maintain records of all approvals granted under this policy and track the status of each activity.

c. The NASA official, at the appropriate level of authority in the supervisory chain over the participating personnel and any applicable non-NASA supervisor (identified by the Review Team per paragraph 1.14.3.h(5) of this NPR), shall sign the approval documentation indicating consent for their assigned personnel to take the risk and participate in the activity.

d. Where deemed applicable by the review, the following NASA officials shall sign the approval documentation indicating that the risks are properly characterized for their area of responsibility and that they concur with acceptance of the risks to personnel under NASA safety responsibility, risk to NASA property, and any public risk due to NASA's part in the activity:

(1) The Center SMA official with cognizance over the activity (mandatory for any activity that involves safety risk to participants, the public, or to NASA property).

(2) The Center Health and Medical official with cognizance over the activity (mandatory for any activity that involves health risk to participants or the public or involves medical equipment or operations as part of the safety risk mitigation strategy).

(3) The NASA General Counsel or Center Chief Counsel (mandatory for any activity that involves U.S. or international law).

(4) The designated Technical Authority(ies) with cognizance over the associated project/program (mandatory for any activity that involves system design changes or invocation of NASA technical requirements as part of the risk mitigation strategy).

e. The personnel participating in the hazardous activity shall sign the approval documentation indicating that they are fully briefed on all safety and health risks inherent in the activity and are willing and able to participate.

f. After signature by the officials/personnel identified in paragraphs 1.14.3.c, 1.14.3.d, and 1.14.3.e of this NPR, the NASA official, at the appropriate level, as identified by the review per paragraph 1.14.3.h.(6) of this NPR, shall sign

the approval documentation indicating formal acceptance of the associated risks to personnel under NASA safety responsibility, risk to NASA property, and any public risk due to NASA's part in the activity.

g. NASA managers (program/project/grant/institutional/other) shall ensure that all aspects of the policy in paragraph 1.14.2 of this NPR are satisfied for applicable work activities under their authority. In accomplishing this, NASA managers shall:

(1) Identify work activities that fall under the applicability of this policy in consultation with the cognizant Center SMA organization.

> Note: Per paragraph 1.14.3a of this NPR, the Chief, Safety and Mission Assurance is responsible for resolving any questions regarding the applicability of this policy to a work activity.

(2) Satisfy local SMA processes and requirements designed to implement this policy.

(3) Establish a Review Team (see paragraph 1.14.3.h of this NPR for Review Team responsibilities) in consultation with the cognizant SMA, Health and Medical, Engineering, and Legal organizations; and ensure that the Review Team incorporates all necessary expertise as required.

(4) Ensure that funding and other resources needed to satisfy this policy are budgeted and allocated.

> Note: This includes any funding needed to staff the Review Team, obtain data, and develop the various review products required by the Review Team, such as the hazards analyses and risk assessments.

(5) Ensure all conditions for NASA approval are met, including implementation of all actions identified by the Review Team.

(6) Ensure the preparation and finalization of the approval documentation.

h. The Review Team established per paragraph 1.14.3.g.(3) of this NPR and program/project/grant/institutional/other personnel as needed shall coordinate to:

(1) Identify and evaluate the safety, health and medical, and any safety-legal aspects of the activity.

(2) Identify and evaluate all associated hazards (design and/or operational), including evaluation of existing hazard/risk mitigations and safety requirements being implemented.

> Note: The extent of this hazard evaluation is determined by the Review Team with the concurrence of the cognizant Center SMA Director and may vary depending on the specific safety concerns associated with the work activity.

(3) Assess and characterize any residual safety risks to personnel, public, and property.

> Note: Characterization of the safety risks may be quantitative or qualitative as determined by the Review Team and as needed to ensure that NASA officials understand any risks they are asked to accept. The basis for the risk assessment includes the current NASA policies, requirements, and standards that would apply if NASA were controlling the activity.

(4) If the initial risks are unacceptable, identify actions that must be implemented to mitigate the risks as conditions for NASA approval to participate.

> Note: This may include implementation of NASA technical standards and/or processes (or portions there of).

(5) Identify the NASA official(s), at the appropriate level of authority in the supervisory chain over the participating personnel and any non-NASA supervisor(s) (in the event that non-NASA personnel are involved), who must consent for the personnel to take the risk and participate in the activity.

> Note: In accomplishing this, the Review Team identifies the appropriate level of NASA management in the supervisory chain with authority to represent the participating personnel based on the risk level and the applicable NASA risk management policy.

(6) Identify the NASA official who must formally accept the risks associated with and grant final approval of the activity.

> Note: In accomplishing this, the Review Team identifies the appropriate level of NASA program/project

management with authority for final approval based on the risk level and the applicable NASA risk management policy.

(7) For a series of related activities (that may involve the same or different participants over a period of time), identify a NASA readiness process to be implemented for each activity.

i. If the Review Team determines that a series of activities is a repetition of, or essentially the same as, a previously reviewed and approved activity, the Review Team may recommend that the NASA approving official (identified per paragraph 1.14.3.h .(6) of this NPR) grant a standing approval that will remain in effect until there are substantive changes in the activity, personnel, or a specified period of time has elapsed, not to exceed 5 years.

j. The Assistant Administrator for Procurement, NASA Grant and Contracting Officers, and Cooperative Agreement, and other agreement officers shall ensure that grants, contracts, and agreements governing activities performed in support of NASA allow for implementation of this policy where specified by the cognizant NASA manager in consultation with the cognizant NASA Center SMA organization (per paragraph 1.14.3.g(1) of this NPR).

| TOC | ChangeLog | Preface | Chapter1 | Chapter2 | Chapter3 | Chapter4 | Chapter5 |
Chapter6 | Chapter7 | Chapter8 | Chapter9 | AppendixA | AppendixB | AppendixC |
AppendixD | AppendixE | AppendixF | AppendixG | ALL |

| NODIS Library | Program Management(8000s) | Search |

DISTRIBUTION:
NODIS

NPR 8715.3D -- Chapter1

This document does not bind the public, except as authorized by law or as incorporated into a contract. This document is uncontrolled when printed. Check the NASA Online Directives Information System (NODIS) Library to verify that this is the correct version before use: https://nodis3.gsfc.nasa.gov.

Page 9 of 9